

(19)日本国特許庁 (J P)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平 1 0 - 6 5 6 6 2

(43)公開日 平成 1 0 年 (1 9 9 8) 3 月 6 日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/08			H04L 9/00	601 C
G11B 20/14	341	9463-5D	G11B 20/14	341 B
H04L 9/14			H04L 9/00	601 E
9/32				641
H04N 7/24				675 A

審査請求 未請求 請求項の数 2 3 O L (全 1 9 頁) 最終頁に続く

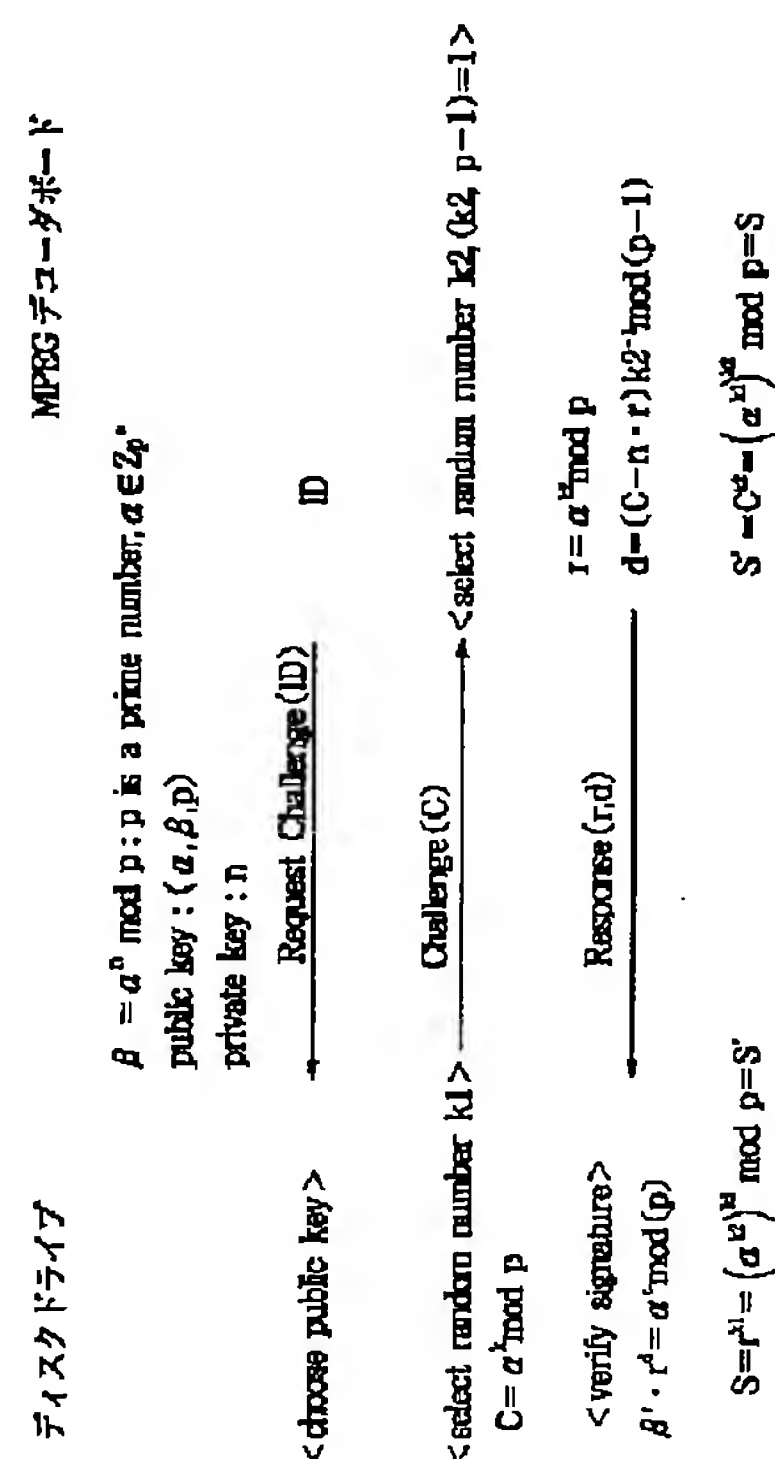
(21)出願番号	特願平 9 - 8 2 5 9 8	(71)出願人	0 0 0 0 0 2 1 8 5 ソニー株式会社 東京都品川区北品川 6 丁目 7 番 3 5 号
(22)出願日	平成 9 年 (1 9 9 7) 4 月 1 日	(72)発明者	石黒 隆二 東京都品川区北品川 6 丁目 7 番 3 5 号 ソ ニー株式会社内
(31)優先権主張番号	特願平 8 - 7 8 6 4 7	(72)発明者	大澤 義知 東京都品川区北品川 6 丁目 7 番 3 5 号 ソ ニー株式会社内
(32)優先日	平 8 (1 9 9 6) 4 月 1 日	(74)代理人	弁理士 稲本 義雄
(33)優先権主張国	日本 (J P)		
(31)優先権主張番号	特願平 8 - 1 4 7 2 7 2		
(32)優先日	平 8 (1 9 9 6) 6 月 1 0 日		
(33)優先権主張国	日本 (J P)		

(54)【発明の名称】データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置

(57)【要約】

【課題】 より安全な復号化方法を実現する。

【解決手段】 M P E G デコーダボードは、メモリに記憶されている I D をディスクドライブに出力する。ディスクドライブは、D V D - R O M に記憶されているキーテーブルから I D に対応する公開鍵を読み出し、この公開鍵を用いて、C h a l l e n g e (C) を演算し、M P E G デコーダボードに出力する。M P E G デコーダボードは、C h a l l e n g e (C) を用いて、デジタルシグニチャ r , d を演算し、ディスクドライブに出力する。ディスクドライブは、デジタルシグニチャ r , d を用いて、暗号化鍵を演算する。また、M P E G デコーダボードは、C h a l l e n g e (C) を用いて、暗号化鍵を演算する。



【特許請求の範囲】

【請求項 1】 所定の暗号化鍵 S を用いてデータを暗号化することにより得られた暗号化データを第 1 の装置から受信し、その暗号化データを前記所定の暗号化鍵 S を用いて復号する第 2 の装置のデータ復号方法において、前記所定の暗号化鍵 S を用いて暗号化された暗号化データを前記第 1 の装置から受信するステップと、

所定の方法により生成された前記所定の暗号化鍵 S を用いて、前記暗号化データを復号するステップとを備え、前記所定の暗号化鍵 S を生成する前記所定の方法においては、

前記第 1 の装置と前記第 2 の装置のうちの一方が、前記第 1 の装置と前記第 2 の装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α , p を選択し、ランダム値 k_1 と前記公開鍵 α , p から、 $C = \alpha k_1 \bmod p$

に従って第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給し、

前記他方が、前記公開鍵 α , p と、ランダム値 k_2 を用いて第 2 のデータ r を演算して、前記一方に供給するとともに、前記第 1 のデータ C と前記ランダム値 k_2 を用いて前記暗号化鍵 S を演算し、

さらに、前記一方が、前記他方から供給される前記第 2 のデータ r と前記ランダム値 k_1 を用いて前記暗号化鍵 S を演算することを特徴とするデータ復号方法。

【請求項 2】 前記第 1 の装置と前記第 2 の装置との間で認証が行われ、前記認証においては、

前記他方が、前記第 1 のデータ C、前記第 2 のデータ r、前記公開鍵 p 、前記ランダム値 k_2 および秘密鍵 n を用いて、第 3 のデータ d を演算して、前記一方に供給し、

前記一方が、前記他方から供給される前記第 2 データ r と前記第 3 のデータ d と所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α , p と前記第 1 のデータ C を用いて演算される値とを比較することを特徴とする請求項 1 に記載のデータ復号方法。

【請求項 3】 前記データは暗号化鍵 Q を用いて暗号化されたデータであり、

前記第 2 の装置は、前記暗号化鍵 S を用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵 x , y を前記第 1 の装置から受信し、

前記所定の暗号化鍵 S を用いて前記暗号化データを復号して前記データを生成し、

前記暗号化された暗号化鍵 x , y を復号して復号された暗号化鍵 Q を生成し、

その復号された暗号化鍵 Q を用いて前記データを復号し、

前記暗号化された暗号化鍵 x , y は、前記暗号化鍵 Q を前記公開鍵 α , β , p を用いて暗号化することにより得

られた鍵であり、

前記暗号化された暗号化鍵 x , y は、秘密鍵 n 及び公開鍵 p を用いて暗号化鍵 Q に復号されることを特徴とする請求項 2 に記載のデータ復号方法。

【請求項 4】 前記公開鍵 α , p は記録媒体から再生されたデータであることを特徴とする請求項 1 に記載のデータ復号方法。

【請求項 5】 所定の暗号化鍵 S を用いてデータを暗号化することにより得られた暗号化データを第 1 の装置から受信し、その暗号化データを前記所定の暗号化鍵 S を用いて復号するデータ復号装置において、

前記所定の暗号化鍵 S を用いて暗号化された暗号化データを前記第 1 の装置から受信する受信手段と、

前記所定の暗号化鍵 S を用いて、前記暗号化データを復号する第 1 の復号手段とを備え、

さらに、前記所定の暗号化鍵 S を生成するために、

前記第 1 の装置と前記復号装置のうちの一方が、前記第 1 の装置と前記復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α , p を選択し、ランダム値 k_1 と前記公開鍵 α , p から、 $C = \alpha k_1 \bmod p$

に従って、第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給する手段と、

前記他方が、前記公開鍵 α , p と、ランダム値 k_2 を用いて第 2 のデータ r を演算して、前記一方に供給するとともに、前記第 1 のデータ C と前記ランダム値 k_2 を用いて前記暗号化鍵 S を演算する手段と、

さらに、前記一方が、前記他方から供給される前記第 2 のデータ r と前記ランダム値 k_1 を用いて前記暗号化鍵 S を演算する手段とを備えることを特徴とするデータ復号装置。

【請求項 6】 前記第 1 の装置と前記データ復号装置との間で認証が行われ、前記認証のために、

前記他方が、前記第 1 のデータ C、前記第 2 のデータ r、前記公開鍵 p 、前記ランダム値 k_2 および秘密鍵 n を用いて、第 3 のデータ d を演算して、前記一方に供給する手段と、

前記一方が、前記他方から供給される前記第 2 のデータ r と前記第 3 のデータ d と所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α , p と前記第 1 のデータ C を用いて演算される値とを比較する手段とを備えることを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 7】 前記データは暗号化鍵 Q を用いて暗号化されたデータであり、

前記復号装置は、

前記暗号化鍵 S を用いて前記データを暗号化することにより得られた、暗号化データ及び前記暗号化された暗号化鍵 x , y を前記第 1 の装置から受信する受信手段と、前記所定の暗号化鍵 S を用いて前記暗号化データを復号して前記データを生成する第 1 の復号手段と、

前記暗号化された暗号化鍵 x , y を復号して復号された暗号化鍵 Q を生成する鍵復号手段と、

その復号された暗号化鍵 Q を用いて前記データを復号する第 2 の復号手段とを有し、

前記暗号化された暗号化鍵 x , y は、前記暗号化鍵 Q を前記公開鍵 α , β , p を用いて暗号化することにより得られた鍵であり、

前記暗号化された暗号化鍵 x , y は、秘密鍵 n 及び公開鍵 p を用いて暗号化鍵 Q に復号されることを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 8】 前記公開鍵 α , p は記録媒体から再生されたデータであることを特徴とする請求項 5 に記載のデータ復号装置。

【請求項 9】 所定の暗号化鍵 S を用いてデータを暗号化して、暗号化データを出力する第 1 の装置と、前記暗号化データを受信して、前記所定の暗号化鍵 S を用いて前記暗号化データを復号するデータ復号装置との間で、前記第 1 の装置と前記データ復号装置の一方が他方を認証する認証方法において、

前記第 1 の装置と前記データ復号装置のうちの一方が、前記第 1 の装置と前記データ復号装置のうちの他方からの識別データを受信して、前記識別データに対応する公開鍵 α , p を選択し、ランダム値 k_1 と前記公開鍵 α , p から、

$$C = \alpha^{k_1} \bmod p$$

に従って、第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給するステップと、

前記他方が、前記公開鍵 α , p と、ランダム値 k_2 を用いて第 2 のデータ r , d を演算して、前記一方に供給するステップと、

前記一方が、前記他方から供給される前記第 2 のデータ r , d と所定の公開鍵 β とを用いて演算される値と、前記公開鍵 α , p と前記第 1 のデータ C を用いて演算される値とを比較するステップとを備えることを特徴とする認証方法。

【請求項 1 0】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、

前記記録媒体は記録データを含んでおり、前記記録データは、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α , p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、

前記データと前記キーテーブルを記録するステップから生成されていることを特徴とする記録媒体。

【請求項 1 1】 前記キーテーブルには、前記第 1 の装置または前記データ復号装置を識別するとき用いられる

公開鍵 β が、さらに、前記識別データに対応して含まれていることを特徴とする請求項 1 0 に記載の記録媒体。

【請求項 1 2】 前記データは暗号化鍵 Q により暗号化されたデータであり、

前記キーテーブルには、前記暗号化鍵 Q を前記公開鍵 α , β , p を用いて暗号化した暗号化鍵 x , y が、さらに前記識別データに対応して含まれていることを特徴とする請求項 1 0 に記載の記録媒体。

【請求項 1 3】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α , p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、

前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項 1 4】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α , p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成する生成手段と、

前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項 1 5】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体において、

前記記録媒体は記録データを含んでおり、前記記録データは、

前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルを生成するステップと、

前記データと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項 1 6】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録方法において、

前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項 17】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生される記録媒体のための記録装置において、

前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成する生成手段と、前記データと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項 18】 暗号鍵 Q で暗号化されたデータを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号し、さらに、暗号化

データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、前記暗号化鍵 Q を、前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと前記暗号化鍵 Q で暗号化されたデータと前記キーテーブルを記録するステップとから生成されていることを特徴とする記録媒体。

【請求項 19】 暗号鍵 Q で暗号化されたデータを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号し、さらに、暗号化

データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、前記暗号化鍵 Q を、前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと

前記暗号化鍵 Q で暗号化されたデータと前記キーテーブルを記録するステップとを備えることを特徴とする記録方法。

【請求項 20】 暗号鍵 Q で暗号化されたデータを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号し、さらに、暗号化

データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成する暗号化手段と、

前記暗号化鍵 Q を、前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と前記暗号化鍵 Q で暗号化されたデータと前記キーテーブルを記録する記録手段とを備えることを特徴とする記録装置。

【請求項 21】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを原盤に記録するステップと、前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項 22】 データを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、前記データと前記キーテーブルを原盤に記録するステップと、

前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【請求項 23】 暗号鍵 Q で暗号化されたデータを所定の暗号化鍵 S を用いて暗号化して、暗号化データを出力

10

20

30

40

50

する第 1 の装置と、前記第 1 の装置からの前記暗号化データを前記暗号化鍵 S を用いて復号し、さらに、暗号化鍵 Q を用いて復号するデータ復号装置とにより構成される再生装置によって再生されるディスクを製造するためのディスク製造方法において、

データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、

前記暗号化鍵 Q を、前記暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、前記第 1 の装置または前記データ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を前記第 1 の装置または前記データ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、

前記暗号化鍵 Q で暗号化されたデータと前記キーテーブルを原盤に記録するステップと、

前記原盤から前記ディスクを生成するステップとを備えることを特徴とするディスク製造方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関し、特に暗号化されているデータを、より安全に復号することができるようにした、データ復号化方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置に関する。

【0002】

【従来の技術】最近、デジタルビデオディスク（以下、DVD と記載する）のフォーマットが統一化されつつあり、統一化された場合、従来のアナログのビデオディスクに代わって普及することが期待されている。この DVD においては、より長時間のビデオデータを記録することができるようにするために、ビデオデータが圧縮符号化（例えば、MPEG（Moving Picture Expert Group）方式、以下、MPEG と記載し、MPEG 方式を用いて説明する）されて記録される。従って、再生時においては、再生データを復号する必要がある。

【0003】ところで、DVD においては、ビデオデータがデジタル的に記録されているため、これを他の記録媒体にコピーすると、ほとんどオリジナルの DVD と遜色のない再生画像が得られる記録媒体を大量に複製することが可能となる。つまり、ディスクドライブと MPEG デコーダとの間でのデータの授受を盗聴され、この盗聴されたデータから不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。また、不正に製造された MPEG デコーダを使用して、ディスクドライブからの再生データを復号し、この不正に復号された不正のスタンパを生成することにより、不正のディスクが大量に複製されることになる。

【0004】このような不正コピーを防止したり、不正に製造された MPEG デコーダを排除するために、ディスクドライブと MPEG デコーダとの間のデータとの授受において、正規の MPEG デコーダであるか否かを認証し、正規の MPEG デコーダであると認証された場合、ディスクドライブから再生データを暗号化鍵を用いて暗号化して、暗号化データを MPEG デコーダに供給する。そして、MPEG デコーダは、この暗号化データを暗号化鍵を用いて復号（解読）し、さらに、復号（解読）された符号化データを復号するようにすることが考えられている。

【0005】したがって、このような対策をとることにより、不正に製造された MPEG デコーダである場合は、ディスクドライブからの再生データが MPEG デコーダに供給されず、不正コピーを防止でき、かつ不正に製造された MPEG デコーダを排除することができる。また、仮に正規の MPEG デコーダを装ってディスクドライブにアクセスされた場合、もしくはディスクドライブと MPEG デコーダとの間でのデータの授受を盗聴された場合に、ディスクドライブからの再生データを得られたとしても、その再生データは暗号化されているため、そのままではそのデータを用いることができない。従って、実質的なコピーを防止することができる。

【0006】

【発明が解決しようとする課題】しかしながら、従来より提案されている単純な暗号化鍵を用いて MPEG デコーダに供給する再生データを暗号化し、MPEG デコーダにおいて、その暗号化された再生データを復号する方法は、暗号化鍵が破られ易いという課題があった。

【0007】本発明はこのような状況に鑑みてなされたものであり、本発明の目的は、デコーダに供給する再生データを破られ難い暗号化鍵を用いて暗号化することにより、不正コピーを確実に防止することができるようにすることにある。

【0008】また、本発明の他の目的は、ディスクドライブからの再生データを暗号化する暗号化鍵の管理を容易にすることができるようにすることにある。

【0009】

【課題を解決するための手段】請求項 1 に記載のデータ復号方法は、所定の暗号化鍵 S を用いて暗号化された暗号化データを第 1 の装置から受信するステップと、所定の方法により生成された所定の暗号化鍵 S を用いて、暗号化データを復号するステップとを備え、所定の暗号化鍵 S を生成する所定の方法においては、第 1 の装置と第 2 の装置のうち的一方が、第 1 の装置と第 2 の装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給し、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第 2 のデ

ータ r を演算して、一方に供給するとともに、第 1 のデータ C とランダム値 k_2 を用いて暗号化鍵 S を演算し、さらに、一方が、他方から供給される第 2 のデータ r とランダム値 k_1 を用いて暗号化鍵 S を演算することを特徴とする。

【0010】請求項 5 に記載のデータ復号装置は、所定の暗号化鍵 S を用いて暗号化された暗号化データを第 1 の装置から受信する受信手段と、所定の暗号化鍵 S を用いて、暗号化データを復号する第 1 の復号手段とを備え、さらに、所定の暗号化鍵 S を生成するために、第 1 の装置と復号装置のうちの一方が、第 1 の装置と復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って、第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給する手段と、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第 2 のデータ r を演算して、一方に供給するとともに、第 1 のデータ C とランダム値 k_2 を用いて暗号化鍵 S を演算する手段と、さらに、一方が、他方から供給される第 2 のデータ r とランダム値 k_1 を用いて暗号化鍵 S を演算する手段とを備えることを特徴とする。

【0011】請求項 9 に記載の認証方法は、第 1 の装置とデータ復号装置のうちの一方が、第 1 の装置とデータ復号装置のうちの他方からの識別データを受信して、識別データに対応する公開鍵 α 、 p を選択し、ランダム値 k_1 と公開鍵 α 、 p から、 $C = \alpha k_1 \bmod p$ に従って、第 1 のデータ C を演算し、その第 1 のデータ C を他方に供給するステップと、他方が、公開鍵 α 、 p と、ランダム値 k_2 を用いて第 2 のデータ r 、 d を演算して、一方に供給するステップと、一方が、他方から供給される第 2 のデータ r 、 d と所定の公開鍵 β とを用いて演算される値と、公開鍵 α 、 p と第 1 のデータ C を用いて演算される値とを比較するステップとを備えることを特徴とする。

【0012】請求項 10 に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップから生成されていることを特徴とする。

【0013】請求項 13 に記載の記録方法は、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【0014】請求項 14 に記載の記録装置は、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第 1 の装置またはデータ復号装置を識別する識別データに対応させ

ることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【0015】請求項 15 に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルを生成するステップと、データとキーテーブルを記録するステップとから生成されていることを特徴とする。

【0016】請求項 16 に記載の記録方法は、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを記録するステップとを備えることを特徴とする。

【0017】請求項 17 に記載の記録装置は、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成する生成手段と、データとキーテーブルを記録する記録手段とを備えることを特徴とする。

【0018】請求項 18 に記載の記録媒体は、記録媒体は記録データを含んでおり、記録データは、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵 Q で暗号化されたデータとキーテーブルを記録するステップとから生成されていることを特徴とする。

【0019】請求項 19 に記載の記録方法は、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと暗号化鍵 Q で暗号化されたデータとキーテーブルを記録するステップとを備えることを特徴とする。

【0020】請求項 20 に記載の記録装置は、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成する暗号化手段と、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成する生成手段と暗号化鍵 Q で暗号化されたデータとキーテーブルを記録する記録手段とを備えることを特徴とする。

【 0 0 2 1 】 請求項 2 1 に記載のディスク製造方法は、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【 0 0 2 2 】 請求項 2 2 に記載のディスク製造方法は、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β を識別データに対応させることにより、キーテーブルデータを生成するステップと、データとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【 0 0 2 3 】 請求項 2 3 に記載のディスク製造方法は、データを暗号化鍵 Q で暗号化して、暗号化鍵 Q で暗号化されたデータを生成するステップと、暗号化鍵 Q を、暗号化鍵 S を演算するとき用いられる公開鍵 α 、 p と、第 1 の装置またはデータ復号装置を識別するとき用いられる公開鍵 β とを用いて暗号化して得られた暗号化鍵 x 、 y を第 1 の装置またはデータ復号装置を識別する識別データに対応させることにより、キーテーブルを生成するステップと、暗号化鍵 Q で暗号化されたデータとキーテーブルを原盤に記録するステップと、原盤からディスクを生成するステップとを備えることを特徴とする。

【 0 0 2 4 】

【発明の実施の形態】 図 1 は、本発明を適用した第 1 の実施の形態のパーソナルコンピュータの構成例を示している。この第 1 の実施の形態において、パーソナルコンピュータ 1 は、ROM タイプのデジタルビデオディスク（以下、DVD-ROM と記載する）2 を駆動するディスクドライブ 1 1 と、ディスクドライブ 1 1 によって再生された再生データが供給され、この再生データをデコードする MPEG デコーダボード 1 2 とから構成されている。MPEG デコーダボード 1 2 からの復号された画像データ（以下、コンテンツデータ (Contents) と記載する）は、モニタ 3 に供給され、モニタ 3 は図示しない表示画面に再生画像を表示するようになっている。

【 0 0 2 5 】 ディスクドライブ 1 1 は、DVD-ROM 2 を駆動し、所定のアクセス点にアクセスすることにより、そこに記録されているデータを再生する駆動部 2 1、駆動部 2 1 からの再生データを暗号化し、その暗号化データを出力する暗号化部 2 2、および、駆動部 2 1 と暗号化部 2 2 を制御する制御部 2 0 から構成されている。DVD-ROM 2 には、所定の位置（例えば最内周トラック）に、暗号化に使用される公開鍵 α 、 β 、 p を含むキーテーブルのデータが予め記録されている。なお、DVD-ROM 2 に記録されているコンテンツデータは、MPEG 方式によって符号化されているデータである。

【 0 0 2 6 】 また、MPEG デコーダボード 1 2 は、パ

ーソナルコンピュータ 1 に対して、適宜装着されるボードであって、暗号化部 2 2 より供給される暗号化データを復号（解読）し、復号（解読）された再生データを出力する復号部 3 1 を有している。この復号部 3 1 は、復号（解読）処理を行うのに必要な秘密鍵 n と、MPEG デコーダボード 1 2 を識別する ID を記憶するメモリ 3 3 を有している。

【 0 0 2 7 】 復号部 3 1 より出力された復号（解読）された再生データは、MPEG デコード部 3 2 に供給され、MPEG デコード部 3 2 は、MPEG 方式に従って復号（解読）された再生データを復号し、コンテンツデータとして出力するようになされている。制御部 3 0 は、復号部 3 1 と MPEG デコード部 3 2 を制御するようになされている。

【 0 0 2 8 】 次に、図 2 と図 3 のフローチャート、図 4 のタイミングチャート及び図 5 の模式図を参照して、図 1 の第 1 の実施の形態の動作について説明する。なお、図 2 は、ディスクドライブ 1 1 の動作を説明するためのフローチャートであり、図 3 は、MPEG デコーダボード 1 2 の動作を説明するフローチャートである。また、図 4 のタイミングチャートは、ディスクドライブ 1 1 と MPEG デコーダボード 1 2 との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図 5 は、ディスクドライブ 1 1 と MPEG デコーダボード 8 2 との間でのデータの流れを示すための模式図である。

【 0 0 2 9 】 DVD-ROM 2 に記録されているデータを再生する場合、最初に、図 3 のステップ S 2 1 において、MPEG デコーダボード 1 2 の制御部 3 0 は、MPEG デコーダボード 1 2 の識別データとしての ID を復号部 3 1 のメモリ 3 3 から読み出し、ディスクドライブ 1 1 の制御部 2 0 に送信する。この ID は、図 4 に示すように、Request Challenge (ID) として、ディスクドライブ 1 1 に送られる。

【 0 0 3 0 】 図 2 のステップ S 1 において、ディスクドライブ 1 1 の制御部 2 0 は、MPEG デコーダボード 1 2 の制御部 3 0 から送られてきた ID を受け取る。そして、制御部 2 0 はステップ S 2 に進み、ステップ S 1 で受け取った ID に対応する公開鍵を、DVD-ROM 2 から読み取るように、駆動部 2 0 を制御する。

【 0 0 3 1 】 すなわち、図 5 に模式的に示すように、DVD-ROM 2 の所定のトラックには、キーテーブルとして、この DVD-ROM 2 を再生して得られる MPEG 方式によって符号化されているコンテンツデータを暗号化する複数の公開鍵 (public key) が、各公開鍵 ($key 1$, $key 2$, $key 3$, ...) が有効であるか否かを表すフラグと共に記録されている。図 5 において、有効な公開鍵 ($key 1$, $key 2$) は○印を付して表し、無効な公開鍵 ($key 3$) は×印を付して表している。DVD-ROM 2 を初めて製造したとき、全て

の公開鍵は有効とされている。しかしながら、例えば、公開鍵の中の所定のもの（図 5 の第 1 の実施の形態の場合、key 3）が第 3 者に破られてしまったような場合、その公開鍵に対応するフラグは、以後、無効として記録される。

【0032】なお、各公開鍵 key 1, key 2, key 3, ... は、それぞれ公開鍵 ($\alpha 1, \beta 1, p 1$), ($\alpha 2, \beta 2, p 2$), ($\alpha 3, \beta 3, p 3$), ... で構成される。

【0033】このような公開鍵と有効フラグを表すキーテーブルが、DVD-ROM 2 の ROM 領域に記録されている場合においては、これを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するとき、キーテーブルの有効フラグだけが書き換えられる。

【0034】制御部 20 は、駆動部 21 を制御し、駆動部 21 は、DVD-ROM 2 の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部 20 に供給され、制御部 20 は、この読み出されたキーテーブルから、ステップ S1 で受け取った ID に対応する公開鍵及びその公開鍵に対応するフラグを検出する。換言すれば、MPEG デコーダボード 12 の正規の製造者に対しては ID が予め与えられており、DVD-ROM 2 の製造者は、各 ID に対応する公開鍵を選定し、テーブルに記憶しておく。そこで、このステップ S2 で、各 ID に対応する公開鍵及びフラグが検出される。

【0035】さらに、ステップ S3 において、制御部 20 は、その公開鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っている MPEG デコーダボード 12 の製造者（ボードメーカー）に割り当てられている ID が発見された場合においては、その ID に対応する公開鍵は無効とされる。そして、その発見後に製造される DVD-ROM 2 には、その公開鍵を無効とするフラグが記録される。ステップ S1 で受け取った ID に対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、MPEG デコーダボード 12 は、DVD-ROM 2 の再生データを受け取ることができないことになる。

【0036】一方、ステップ 3 において、ステップ S1 で受け取った ID に対応する公開鍵が有効であると判定された場合、ステップ S4 に進み、制御部 20 は、次式 (1) から Challenge (C) を計算し、図 4 に示すように、この Challenge (C) として MPEG デコーダボード 12 の制御部 30 に供給する。

$$C = \alpha k1 \bmod p \cdots (1)$$

【0037】ここで、 α , p は、DVD-ROM 2 のキーテーブルに記録されている公開鍵であり、 p は素数で

ある。また、 $k1$ は、適宜選択されるランダムな番号（値）である。また、 $A \bmod B$ は、 A を B で割算したとき得られる剰余を表している。

【0038】上述した式 (1) は、トラップドアファンクションの関数（離散対数問題）として知られており、 $k1$ から C は容易に計算できるが、 C から $k1$ を計算することができる関数は知られていない。

【0039】図 4 に示すように、このようにして計算された Challenge (C) は、MPEG デコーダボード 12 の制御部 30 に供給される。制御部 30 は、図 3 のステップ S22 において、この Challenge (C) を受け取る。そして、制御部 30 は、ステップ S23 に進み、所定のランダムな番号 $k2$ を選択し、次式 (2)、(3) からデジタルシグニチャ r, d を演算し、その結果を Response (r, d) として、ディスクドライブ 11 に供給する。

$$r = \alpha k2 \bmod p \cdots (2)$$

$$d = (C - n \cdot r) k2^{-1} \bmod (p - 1) \cdots (3)$$

【0040】なお、このランダムな値 $k2$ は、 $p - 1$ と素の関係にある。

【0041】図 4 に示すように、上述した式 (2) 及び (3) から求められたデジタルシグニチャ r, d は、Response (r, d) として、ディスクドライブ 11 の制御回路 20 に供給される。制御部 20 は、図 2 のステップ S5 において、この Response (r, d) を受け取り、ステップ S6 に進み、ステップ 6 において、この Response (r, d) 内のデジタルシグニチャ r, d をチェックする。

【0042】すなわち、制御部 20 は、図 4 に示すように、 $\beta r \cdot r d$ を演算するとともに、 $\alpha C \bmod (p)$ を演算し、両者の値が等しいか否かを判定する。MPEG デコーダボード 12 が、正規のデコーダである場合、デジタルシグニチャ r, d と公開鍵 β とを用いて演算される値 $\beta r \cdot r d$ の値は、Challenge (C)、公開鍵 α , p を用いて求められる値 $\alpha C \bmod (p)$ の値と等しくなる。

この 2 つの演算値が等しくなることは、El Gamal Signature Scheme として、よく知られている (A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 21 (1985), 469-472)。

逆に、MPEG デコーダボード 12 が正規のデコーダではない場合、両者の値は異なるものとなる。この場合、処理は終了される。従って、この場合、DVD-ROM 2 の再生データは MPEG デコーダボード 12 に出力されないことになる。なお、ここまでのデータの授受の流れが、図 5 に示される Key Exchange に対応している。

【0043】ステップ S6 において、演算された 2 つの値が等しいと判定された場合、ステップ S7 に進み、制御部 20 は、Session key (S) を次式 (4) より演算す

る (図 5 の Session Key S)。

$$S = r k_1 \cdots (4)$$

【0044】一方、MPEGデコーダボード12の制御部30は、図3のステップS23において、Response (r, d) を計算して、ディスクドライブ11に供給した後、ステップS24に進み、ステップS22で受け取ったChallenge (C) を用いて次式(5)に従って、Session key (S*) を演算する (図5のSession Key S*)。

$$S' = C k_2 \cdots (5)$$

【0045】図2のフローチャートのステップS7において、ディスクドライブ11の制御部20によって計算されたSession Key Sと、図3のフローチャートのステップS24においてMPEGデコーダボード12の制御部30によって演算されたSession Key S' は、それぞれ次式(6)及び(7)で表され、両者は等しい値となる。すなわち、ディスクドライブ11とMPEGデコーダボード12において、それぞれ同一の暗号化鍵が得られたことになる。

$$S = r k_1 = (\alpha k_2) k_1 \bmod p \cdots (6)$$

$$S' = C k_2 = (\alpha k_1) k_2 \bmod p \cdots (7)$$

【0046】このことは、Diffie-Hellman Key Exchangeにおいて知られている (Diffie-Hellman W. Diffie and M. E. Hellman, Multiuser cryptographic techniques, A FIPS Conference Proceedings, 45(1976), 102-112)。

【0047】そこで、ディスクドライブ11の制御部20は、ステップS8に進み、駆動部21にDVD-ROM2を駆動させるとともに、ステップS7で求めたSession Key Sを暗号化部22に供給する。そして、駆動部21は、DVD-ROM2の所定の位置から記録されているデータを再生する。暗号化部22は、駆動部21でDVD-ROM2から再生された再生データをステップS7で求めたSession Key Sを用いて暗号化して、暗号化データを生成する。そして、この暗号化データは、MPEGデコーダボード12に供給される (図5のEncryption)。

【0048】MPEGデコーダボード12の復号部31は、図3のステップS25で、暗号化部22から供給された暗号化データを受け取り、ステップS26において、その暗号化データを、ステップS24で求めたSession Key S' を用いて復号 (解読) する (図5のDecryption)。上述したように、Session Key S' は、セッションキーSと同一の値であるので、正しい復号 (暗号の解読) を行うことができる。そして、この復号 (解読) された再生データ (符号化されているコンテンツデータ) がMPEGデコード部32に供給される。

【0049】MPEGデコード部32は、復号部31によって復号 (解読) された符号化されているコンテンツデータを受け取り、MPEG方式で符号化されているその復号 (解読) されたコンテンツデータを復号し、この

復号されたコンテンツデータをモニタ3に供給する (図5のDecode)。そして、モニタ3は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【0050】上述したように、第1の実施の形態においては、公開鍵を使用し、この公開鍵をディスクに記録しておくこと、公開鍵の配布が容易となる。また、公開鍵を複数記録しておけば、MPEGデコーダボード12の製造者 (ボードメーカー) に秘密鍵を配布するとき、ボードメーカー毎に異なる鍵を割り当てることができる。よって、1つのボードメーカーの秘密鍵が破られた場合でも、他のボードメーカーには別の秘密鍵が割り当てられているため、他のボードメーカーの秘密鍵はそのまま使用でき、被害を最小限に食い止めることができる。

【0051】さらに、ディスクドライブ11において、秘密鍵nはもとより、公開鍵 α , β , pを保持しておく必要がないので、ディスクドライブにおける管理が容易となる。

【0052】なお、ディスクドライブ内の制御部20は、暗号化部22と一体化して構成してもよい。また、MPEGデコーダボード内の制御部30は、復号部31と一体化して構成してもよい。

【0053】また、以上の第1の実施の形態においては、MPEGデコーダボード12からIDをディスクドライブ11に供給し、ディスクドライブ11において認証を行うようにしたが、ディスクドライブ11からIDを供給し、MPEGデコーダボード12において認証を行うようにしてもよい。また、ディスクとして、DVD-ROMを用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクがRAMタイプのディスクである場合、制御部20は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【0054】図6は、以上の第1の実施の形態におけるDVD-ROM2に対してデータを記録する記録装置の構成例を示している。図6に示すように、合成部51は、ID供給源41からのID、フラグ供給源42からのフラグ、および公開鍵供給源43からの公開鍵 α , β , pをキーテーブル (Key Table) のデータとして合成し、その合成されたデータを合成部52に供給する。また、コンテンツデータ供給源44からのビデオデータ等のコンテンツデータ (Contents) がMPEGエンコード部53に供給され、MPEGエンコード部53は、コンテンツデータをMPEG方式に従って符号化し、符号化されたコンテンツデータを合成部52に供給する。合成部52は、合成部51より入力されたキーテーブルのデータと、MPEGエンコード部53からの符号化されたコンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤54に記録される。さらに、その原盤54から大量のレプリカとしての

DVD-ROM 2 が生成される。これにより、DVD-ROM 2 には、コンテンツデータの他、各 ID に対応したフラグ及び公開鍵からなるキーテーブルが記録される。

【0055】次に、本発明を適用した第 2 の実施の形態について説明する。なお、第 2 の実施の形態を説明するにあたり、まず、コンテンツデータを DVD-ROM に記録する記録装置を説明した後、パーソナルコンピュータの構成を説明する。

【0056】図 7 は、第 2 の実施の形態における DVD-ROM 7 2 に対してデータを記録する記録装置の構成例を示している。この第 2 の実施の形態においては、コンテンツデータが暗号化され、暗号化コンテンツデータが DVD-ROM 7 2 に記録されるようになされている。

【0057】コンテンツ情報源 6 1 からのコンテンツデータは、MPEG エンコード部 6 9 に供給される。MPEG エンコード部 6 9 は、コンテンツデータを MPEG 方式に従って符号化し、符号化コンテンツデータを暗号化部 6 2 に供給する。また、暗号化鍵供給源 6 3 からの暗号化鍵 Q が暗号化部 6 2 に供給される。暗号化部 6 2 は、暗号化鍵 Q を用いて、例えば、符号化コンテンツデータを DES (Data Encryption Standard) 方式に従って暗号化し、暗号化コンテンツデータを合成部 7 0 に供給する。

【0058】一方、この暗号化鍵 Q は、暗号化鍵暗号化部 6 4 にも供給される。また、公開鍵供給源 6 7 からの公開鍵 α 、 β 、 p が暗号化鍵暗号化部 6 4 に供給され、暗号化鍵暗号化部 6 4 は、次式 (8) 及び (9) に従って、公開鍵 α 、 β 、 p を用いて、暗号化鍵 Q を暗号化し、暗号化された暗号化鍵 x 、 y を生成する。

$$x = \alpha k^3 \bmod (p) \quad \cdots (8)$$

$$y = Q \cdot \beta k^3 \bmod (p) \quad \cdots (9)$$

ここで、 k^3 は、適宜選択されるランダムな番号 (値) である。

【0059】また、合成部 6 8 は、ID 供給源 6 5 からの ID、フラグ供給源 6 6 からのフラグ、公開鍵供給源 6 7 からの公開鍵 α 、 β 、 p 、並びに暗号化部 6 4 からの暗号化された暗号化鍵 x 、 y を合成し、キーテーブルとして合成部 7 0 に供給する。合成部 7 0 は、合成部 6 8 から供給されたキーテーブルのデータと、暗号化部 6 2 からの暗号化コンテンツデータを合成して、記録データとして出力する。そして、この記録データが原盤 7 1 に記録される。さらに、その原盤 7 1 から大量のレプリカとしての DVD-ROM 7 2 が製造される。これにより、図 7 に示すように、DVD-ROM 7 2 には、暗号化コンテンツデータの他に、各 ID に対応したフラグ、公開鍵 $key_i (\alpha_i, \beta_i, p_i)$ 、並びに暗号化された暗号化鍵 (x_i, y_i) が、キーテーブルとして記録される。

【0060】次に、上述したような方法で製造された DVD-ROM 7 2 に記録されているデータを再生する第 2 の実施の形態のパーソナルコンピュータの構成について説明する。図 8 は、本発明を適用した第 2 の実施の形態のパーソナルコンピュータの構成例を示している。パーソナルコンピュータ 8 0 は、DVD-ROM 7 2 をドライブするディスクドライブ 8 1 と、ディスクドライブ 8 1 によって再生された再生データが供給され、この再生データをデコードする MPEG デコーダボード 8 2 から構成されている。MPEG デコーダボード 8 2 からの復号されたコンテンツデータは、モニタ 7 3 に供給され、モニタ 7 3 は、図示しない表示画面に再生画像を表示するようになされている。この場合におけるディスクドライブ 8 1 と MPEG デコーダボード 8 2 の構成は、基本的に図 1 に示す場合と同様である。

【0061】ディスクドライブ 8 1 は、DVD-ROM 7 2 を駆動し、所定のアクセス点にアクセスして、そこに記録されているデータを再生する駆動部 9 1、駆動部 9 1 から再生データを暗号化し、その暗号化データを入力する暗号化部 9 2、及び駆動部 9 1 と暗号化部 9 2 を制御する制御部 9 0 から構成されている。DVD-ROM 7 2 には、所定の位置 (例えば最内周トラック) に、暗号化に使用される公開鍵 α 、 β 、 p 及び暗号化された暗号化鍵 x 、 y を含むキーテーブルのデータが予め記録されている。なお、DVD-ROM 7 2 に記憶されているコンテンツデータは、MPEG 方式によって符号化されているデータである。

【0062】また、MPEG デコーダボード 8 2 は、第 1 の実施の形態と同様に、パーソナルコンピュータ 8 0 に対して、適宜装着されるボードであって、暗号化部 9 2 より供給される暗号化データを復号 (解読) し、その復号 (解読) された暗号化コンテンツデータを出力する復号部 1 0 1 を有している。この復号部 1 0 1 は、復号 (解読) 処理を行うために必要な秘密鍵 n と、MPEG デコーダボード 8 2 を識別する ID を記憶するメモリ 1 0 3 を有している。

【0063】復号部 1 0 1 から出力された復号された暗号化コンテンツデータは、復号部 1 0 4 に供給される。また、暗号化鍵復号部 1 0 5 は、ディスクドライブ 8 1 の駆動部 9 1 からの暗号化された暗号化鍵 x 、 y を受け取り、秘密鍵 n と公開鍵 p を用いてこの暗号化鍵 Q を復号 (解読) し、この復号された暗号化鍵 Q を復号鍵として復号部 1 0 4 に供給する。そして復号部 1 0 4 は、この復号鍵を用いて暗号化コンテンツデータを復号 (解読) し、復号 (解読) された符号化コンテンツデータは、MPEG デコード部 1 0 2 に供給され、MPEG 方式によって復号され、コンテンツデータとして出力されるようになされている。制御部 1 0 0 は、復号部 1 0 1、MPEG デコーダ部 1 0 2、復号部 1 0 4 及び暗号化鍵復号部 1 0 5 を制御する。

【0064】次に、図9と図10のフローチャート、図11のタイミングチャート、及び図12の模式図を参照して、その動作について説明する。図9は、図8のディスクドライブ81の処理を説明するフローチャートであり、図10は、図8のMPEGデコーダボード82の動作を説明するフローチャートである。また、図11のタイミングチャートは、ディスクドライブ81とMPEGデコーダボード82との間において授受されるデータと、各データに対応して実行される演算を表している。さらに、図12は、ディスクドライブ81とMPEGデコーダボード82との間のデータの流れを示すための模式図である。

【0065】DVD-ROM72に記録されているデータを再生する場合、最初に図10のステップS51において、MPEGデコーダボード82の制御部100は、MPEGデコーダボードの識別データとしてのIDを復号部101のメモリ103から読み出し、ディスクドライブ81の制御部90に送信する。このIDは、図11に示すように、Request Challenge (ID) としてディスクドライブ81に送られる。

【0066】ディスクドライブ81の制御部90は、MPEGデコーダボード82の制御部100から送られてきたIDを図9のステップS31において受け取る。そして、制御部90はステップS32に進み、ステップS31で受け取ったIDに対応する公開鍵を、DVD-ROM72から読み取るように、駆動部91を制御する。

【0067】すなわち、図12に模式的に示されるように、DVD-ROM72の所定のトラックには、キーテーブルとして、コンテンツデータを暗号化した暗号化鍵Qを公開鍵を用いて暗号化した暗号化された暗号化鍵x、yと、このDVD-ROM72を再生して得られるMPEG方式によって符号化されているコンテンツデータを暗号化する公開鍵(public key)とが、各公開鍵(key1, key2, key3, ……)及び暗号化された暗号化鍵((x1, y1), (x2, y2), (x3, y3) ……)が有効であるか否かを表すフラグと共に記録されている。

【0068】図12において、有効な公開鍵(key1, key2)及び暗号化された暗号化鍵((x1, y1), (x2, y2))は○印を付して表し、無効な公開鍵(key3)及び暗号化された暗号化鍵(x3, y3)は×印を付して表している。DVD-ROM72を初めて製造したとき、全ての公開鍵及び暗号化鍵Qは有効とされている。しかしながら、例えば、公開鍵及び暗号化鍵Qの中の所定のもの(図12の第2の実施の形態の場合、key3及び(x3, y3)に対応する暗号化鍵Q)が第3者に破られしまったような場合、その公開鍵及び暗号化鍵Qに対応するフラグは無効として記録される。

【0069】なお、各公開鍵key1, key2, key

y3, ……は、それぞれ公開鍵($\alpha 1$, $\beta 1$, p1), ($\alpha 2$, $\beta 2$, p2), ($\alpha 3$, $\beta 3$, p3), ……で構成されている。

【0070】このような公開鍵、暗号化された暗号化鍵Q及び有効フラグを表すキーテーブルが、DVD-ROM72のROM領域に記録されている場合には、このデータを書き換えることができないため、新しいバージョンのディスクとして、実質的に同一のコンテンツデータが記録されているディスクを新たに製造するときに、キーテーブルの有効フラグだけが書き換えられる。

【0071】制御部90は、駆動部91を制御し、駆動部91は、DVD-ROM72の所定のトラックに記録されているキーテーブルを読み出す。そして、この読み出したキーテーブルは制御部90に供給され、制御部90は、この読み出されたキーテーブルから、ステップS31で受け取ったIDに対応する公開鍵、暗号化された暗号化鍵及びそれらに対応するフラグを検出する。換言すれば、MPEGデコーダボード82の正規の製造者(ボードメーカー)に対してはIDが予め与えられており、DVD-ROM72の製造者は、各IDに対応する公開鍵及び暗号化鍵Qを選定して、その公開鍵と公開鍵によって暗号化された暗号化鍵x, yをテーブルに記憶しておく。そこで、このステップS32で、各IDに対応する公開鍵及び暗号化された暗号化鍵x, yが検出される。

【0072】さらに、ステップS33において、この公開鍵及び暗号化された暗号化鍵に対応するフラグが有効とされているか否かを判定する。上述したように、例えば、不正コピーを行っているMPEGデコーダボード82の製造者(ボードメーカー)に割り当てられているIDが発見された場合においては、そのIDに対応する公開鍵は無効とされる。そして、その発見後に製造されるDVD-ROM72に対応する公開鍵及び暗号化鍵Qを無効とするフラグが記録される。ステップS31で受け取ったIDに対応する公開鍵が無効と判定された場合、処理が終了される。すなわち、この場合においては、MPEGデコーダボード82は、DVD-ROM72の再生データを受け取ることができないことになる。なお、ここまでのデータの授受の流れが、図12に示されるKey exchangeに対応している。

【0073】一方、ステップ33において、ステップ31で受け取ったIDに対応する公開鍵が有効であると判定された場合、ステップS34に進み、制御部90は、第1に実施の形態と同様に、上述した式(1)からChallenge(C)を計算し、MPEGデコーダボード82の制御部100に供給する。

【0074】図12に示すように、このようにして計算されたChallenge(C)は、MPEGデコーダボード82の制御部100に供給される。制御部100は、図10のステップS52において、このChallenge(C)を

受け取る。そして、制御部 1 0 0 は、ステップ S 5 3 に進み、第 1 の実施の形態と同様に、所定のランダムな番号 k_2 を選択し、上述した式 (2)、(3) からデジタルシグニチャ r, d を演算し、その結果を Response

(r, d) として、ディスクドライブ 8 1 に供給する。

【0075】図 1 1 に示すように、上述した式 (2) 及び (3) から求められたデジタルシグニチャ r, d は、Response (r, d) として、ディスクドライブ 8 1 の制御回路 9 0 に供給される。制御部 9 0 は、図 9 のステップ S 3 5 において、この Response (r, d) を受け取り、ステップ S 3 6 に進み、ステップ 3 6 において、この Response (r, d) 内のデジタルシグニチャ r, d をチェックする。

【0076】すなわち、制御部 9 0 は、図 1 2 に示すように、 $\beta r \cdot r d$ を演算するとともに、 $\alpha C \bmod (p)$ を演算し、両者の値が等しいか否かを判定する。MPEG デコーダボード 8 2 が、正規のデコーダである場合、第 1 の実施の形態と同様に、デジタルシグニチャ r, d と公開鍵 β とを用いて演算される値 $\beta r \cdot r d$ の値は、Challenge (C)、公開鍵 α, p を用いて求められる値 $\alpha C \bmod (p)$ の値と等しくなる。逆に、MPEG デコーダボード 1 2 が正規のデコーダではない場合、両者の値は異なるものとなる。この場合、制御部 9 0 の処理は終了される。従って、この場合、DVD-ROM 7 2 のビデオデータは MPEG デコーダボード 8 2 に出力されないことになる。

【0077】ステップ S 3 6 において、演算された 2 つの値が等しいと判定された場合、ステップ S 3 7 に進み、制御部 9 0 は、第 1 の実施の形態と同様に、Session Key S を上述した式 (4) より演算する (図 1 2 の Session Key S)。

【0078】一方、MPEG デコーダボード 8 2 の制御部 9 0 は、図 1 0 のステップ S 5 3 において、Response (r, d) を計算して、ディスクドライブ 8 1 に供給した後、ステップ S 5 4 に進み、第 1 の実施の形態と同様に、ステップ S 5 2 で受け取った Challenge (C) を用いて上述した式 (5) に従って、Session Key S' を演算する (図 1 2 の Session Key S')。

【0079】よって、ステップ S 3 7 においてディスクドライブ 8 1 の制御部 9 0 によって計算された Session Key S と、ステップ S 5 4 において MPEG デコーダボード 8 2 の制御部 1 0 0 によって演算された Session Key S' は、第 1 の実施の形態で説明したように、それぞれ上述した式 (6) 及び (7) で表され、両者は等しい値となる。すなわち、ディスクドライブ 8 1 と MPEG デコーダボード 8 2 において、それぞれ同一の暗号化鍵が得られたことになる。

【0080】さらに、ディスクドライブ 1 1 において、Session Key S を演算すると、ステップ S 3 8 に進み、駆動部 9 1 は、DVD-ROM 7 2 より再生された暗号

化された暗号化鍵 x, y を、そのまま MPEG デコーダボード 8 2 に供給する (図 1 2 の x, y (as is))。

【0081】MPEG デコーダボード 8 2 の制御部 1 0 0 は、Session Key S' が得られたら、次にステップ S 5 5 に進み、ステップ 3 8 において、暗号化鍵復号部 1 0 5 がディスクドライブ 8 1 か供給された暗号化された暗号化鍵 x, y を受け取るように制御し、また、メモリ 1 0 3 から秘密鍵 n を読み出して、暗号化鍵復号部 1 0 5 に供給し、次に、ステップ S 5 6 に進む。ステップ 5 6 において、暗号化鍵復号部 1 0 5 は、暗号化された暗号化鍵 x, y を次式 (10) に従って復号 (解読) し、この復号された暗号化鍵 Q (復号鍵) が復号部 1 0 4 に供給される (図 1 2 の Key Decryption)。

$$Q = (y / x^n) \bmod (p) \quad \dots (10)$$

【0082】すなわち、暗号化鍵復号部 1 0 5 は、秘密鍵 n と公開鍵 p を用いて、暗号化された x, y から暗号化鍵 Q を復号 (解読) する。

【0083】一方、ディスクドライブ 8 1 は、ステップ S 3 8 で暗号化された暗号化鍵 x, y を MPEG デコーダボード 8 2 に供給した後、さらに、ステップ S 3 9 に進み、制御部 9 0 は、駆動部 9 1 を制御して、駆動部 9 1 は、DVD-ROM 7 2 から暗号化コンテンツデータを再生し、その再生された暗号化コンテンツデータ (暗号化鍵 Q で暗号化されているコンテンツ) を暗号部 9 2 に供給するとともに、制御部 9 0 は、ステップ S 3 7 で求めた Session Key S を暗号化部 9 2 に供給する。暗号化部 9 2 は、再生された暗号化コンテンツデータを Session Key S で暗号化して、暗号化データを MPEG デコーダボード 8 2 に供給する (図 1 2 の Encryption)。

【0084】MPEG デコーダボード 8 2 の復号部 1 0 1 は、図 1 0 のステップ S 5 5 において、暗号化部 9 2 から供給された暗号化データを受け取り、ステップ S 5 6 において、その暗号化データを、ステップ S 5 4 で求めた Session Key S' を用いて復号 (解読) する (図 1 2 の Decryption)。上述したように、Session Key S' は、Session Key S と同一の値であるので、正しい復号 (暗号の解読) を行うことができる。これにより、Session Key S による暗号化が解除され、暗号化鍵 Q で暗号化されている暗号化コンテンツデータが得られることになる。そして、この暗号化コンテンツデータが復号部 1 0 4 に供給される。

【0085】次にステップ S 5 9 に進み、復号部 1 0 4 は、復号部 1 0 1 からの暗号化コンテンツデータを復号部 1 0 4 からの復号 (解読) された暗号化鍵 Q (復号鍵) を用いて復号 (解読) する。すなわち、第 2 の実施の形態の場合、DES の復号処理が実行される (図 1 2 の Decryption)。そして、この復号 (解読) された符号化されているコンテンツデータ (符号化コンテンツデータ) が MPEG デコード部 1 0 2 に供給される。

【0086】MPEG デコード部 1 0 2 は、復号部 1 0

4 によって復号（解読）された符号化コンテンツデータを受け取り、この符号化コンテンツデータを M P E G 方式で復号し、この復号されたコンテンツデータをモニタ 3 に供給する（図 1 2 の Decode）。そして、モニタ 7 3 は、このコンテンツデータを再生画像として図示しない表示画面に表示する。

【 0 0 8 7 】以上、上述したように、第 2 の実施の形態においては、ディスクに記録されているコンテンツデータが暗号化されており、さらに、ディスクドライブ 8 1 において、このコンテンツデータが暗号化される（つまり、コンテンツデータが 2 重に暗号化されている）ため、ディスクドライブ 8 1 と M P E G デコーダボード 8 2 間のデータを傍受したとしても、第 1 の実施の形態の効果に比べて、不正コピーはより困難になる。

【 0 0 8 8 】また、このように、この第 2 の実施の形態においては、セッションキー S を求めるとき用いられる公開鍵 α 、 p と、認証処理（識別処理）を行うとき用いられる公開鍵 β とを用いて、コンテンツを暗号化する暗号化鍵 Q を暗号化するようにしたので、暗号化のために必要となる鍵の数を減らすことができる。すなわち、暗号化鍵 Q を、公開鍵 α 、 β 、 p 以外の鍵を用いて暗号化することも可能であるが、そのようにすると鍵の数が増加し、鍵が破られた場合において、鍵を変更する（無効とする）処理が困難になる。そこで、この第 2 の実施の形態のように、セッションキー S と認証に用いられる公開鍵 α 、 β 、 p を、コンテンツを暗号化する暗号化鍵 Q の暗号化にも共通に用いるようにすることにより、鍵の数を減らすことができる。

【 0 0 8 9 】また、第 2 に実施の形態において、ディスクドライブ内の制御部 9 0 は、暗号化部 9 2 と一体化して構成してもよい。また、M P E G デコーダボード内の制御部 1 0 0 は、復号部 1 0 1、1 0 4 及び 1 0 5 と一体化して構成してもよい。

【 0 0 9 0 】さらに、第 2 の実施の形態においては、M P E G デコーダボード 8 2 から I D をディスクドライブ 8 1 に供給し、ディスクドライブ 8 1 において認証を行うようにしたが、ディスクドライブ 8 1 から I D を供給し、M P E G デコーダボード 8 2 において認証を行うようにしてもよい。また、ディスクとして、D V D - R O M を用いる場合を例としたが、本発明は、その他の記録媒体に記録されているデータを再生する場合にも適用することができる。なお、ディスクが R A M タイプのディスクである場合、制御部 9 0 は、所定の指令が入力されたとき、そのフラグを無効なフラグに書き換えることも可能である。

【 0 0 9 1 】なお、上記第 1 及び第 2 の実施の形態においては、図 6、図 7、図 1 2 に示すように、暗号化された公開鍵 x 、 y を、公開鍵 α 、 β 、 p とともにまとめて 1 つのキーテーブルに登録するようにしたが、例えば図 1 3 に示すように、暗号化された暗号化鍵 x 、 y を、フ

ラグとともに I D に対応して、公開鍵 α 、 β 、 p のキーテーブルとは別のキーテーブルにまとめるようにすることも可能である。

【 0 0 9 2 】さらに、上記第 1 及び第 2 の実施の形態においては、上記した鍵の生成に 1 方向性関数を用いるようにすることが可能である。この 1 方向性関数を用いて鍵の生成方法は、本出願人によって、例えば、特願平 8 - 2 6 9 5 0 2 号として先に提案されているものを用いることができる。

10 【 0 0 9 3 】以上、上記第 1 及び第 2 の実施の形態においては、本発明をディスクドライブとデコーダとの間における暗号化鍵の交換と認証を例として説明したが、本発明はこれに限らず、その他の装置に適用することも可能である。例えば、ディスクドライブを、ネットワークを介してデコーダにデータを伝送するセンタに置き換え、センタとデコーダの間において、本発明を適用することもできる。

20 【 0 0 9 4 】また、上記第 1 及び第 2 の実施の形態においては、記録されるコンテンツデータの一例として、ビデオデータを用いて説明しているが、本発明はこれに限らず、オーディオデータ、プログラムデータもしくはその他のデータに適用することが可能である。

【 0 0 9 5 】さらに、上記第 1 及び第 2 の実施の形態においては、M P E G 方式のエンコーダ及びデコーダを例として説明したが、本発明はこれに限らず、他の符号化方式によるエンコーダ及びデコーダを適用することも可能である。

30 【 0 0 9 6 】また、本発明の第 1 及び第 2 の実施の形態は、ブロック図を用いてハードウェアとして表現しているが、本発明はこれに限らず、C P U やメモリなどを用いてソフトウェアで実現することも可能である。

【 0 0 9 7 】なお、本発明の主旨を逸脱しない範囲において、さまざまな変形や応用例が考えうる。従って、本発明の要旨は、実施の形態に限定されるものではない。

【 0 0 9 8 】

40 【発明の効果】以上、上述したように、本発明におけるデータ復号方法およびデータ復号装置によれば、一方は、他方から供給されるデジタルシグニチャ r とランダムな値 $k 1$ を用いて暗号化鍵を演算し、他方は、チャレンジ C とランダムな値 $k 2$ を用いて暗号化鍵を演算するようにし、このデジタルシグニチャ r を公開鍵 α 、 p とランダムな値 $k 2$ を用いて演算するようにしたので、暗号化鍵が破られ難くなり、データの不正なコピーを確実に防止することが可能となる。

50 【 0 0 9 9 】また、本発明における認証方法によれば、デジタルシグニチャ r 、 d と、所定の公開鍵 β とを用いて演算される値と、公開鍵 α 、 p とチャレンジ C を用いて演算される値とを比較して、その比較結果に対応して認証を行うようにしたので、より安全な認証システムを構築することが可能となる。

【0100】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び記録装置によれば、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p を、第1の装置または第2の装置を識別する識別データに対応して記録媒体に記録するようにしたので、データの不正なコピーを確実に防止することが可能な記録媒体を実現することができる。

【0101】また、本発明における記録媒体、ディスクの製造方法、記録方法及び記録装置によれば、第1の装置または第2の装置を識別するとき用いられる公開鍵 β を、識別データに対応して記録媒体に記録するようにしたので、より安全な認証システムを構築することが可能な記録媒体を実現することができる。

【0102】さらに、本発明における記録媒体、ディスク製造方法、記録方法及び請求項18に記載の記録装置によれば、データを暗号化する暗号化鍵Qを、暗号化鍵Sを演算するとき用いられる公開鍵 α 、 p と、第1の装置または第2の装置を識別するとき用いられる公開鍵 β とを用いて暗号化した暗号化鍵 x 、 y を、第1の装置または第2の装置を識別する識別データに対応して記録する

【図面の簡単な説明】

【図1】本発明を適用した第1の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

【図2】図1のディスクドライブの動作を説明するフローチャートである。

【図3】図1のMPEGデコーダボードの動作を説明するフローチャートである。

【図4】図1の第1の実施の形態の動作を説明するタイミングチャートである。

【図5】図1の第1の実施の形態におけるデータの流れを説明する模式図である。

【図6】本発明を適用した第1の実施の形態におけるDVD-ROMを製造する装置の構成例を示すブロック図である。

【図7】本発明を適用した第2の実施の形態におけるDVD-ROMを製造する装置の構成例を示すブロック図である。

【図8】本発明を適用した第2の実施の形態のパーソナルコンピュータの構成例を示すブロック図である。

【図9】図8のディスクドライブの動作を説明するフローチャートである。

【図10】図8のMPEGデコーダボードの動作を説明するフローチャートである。

【図11】図8の第2の実施の形態の動作を説明するタイミングチャートである。

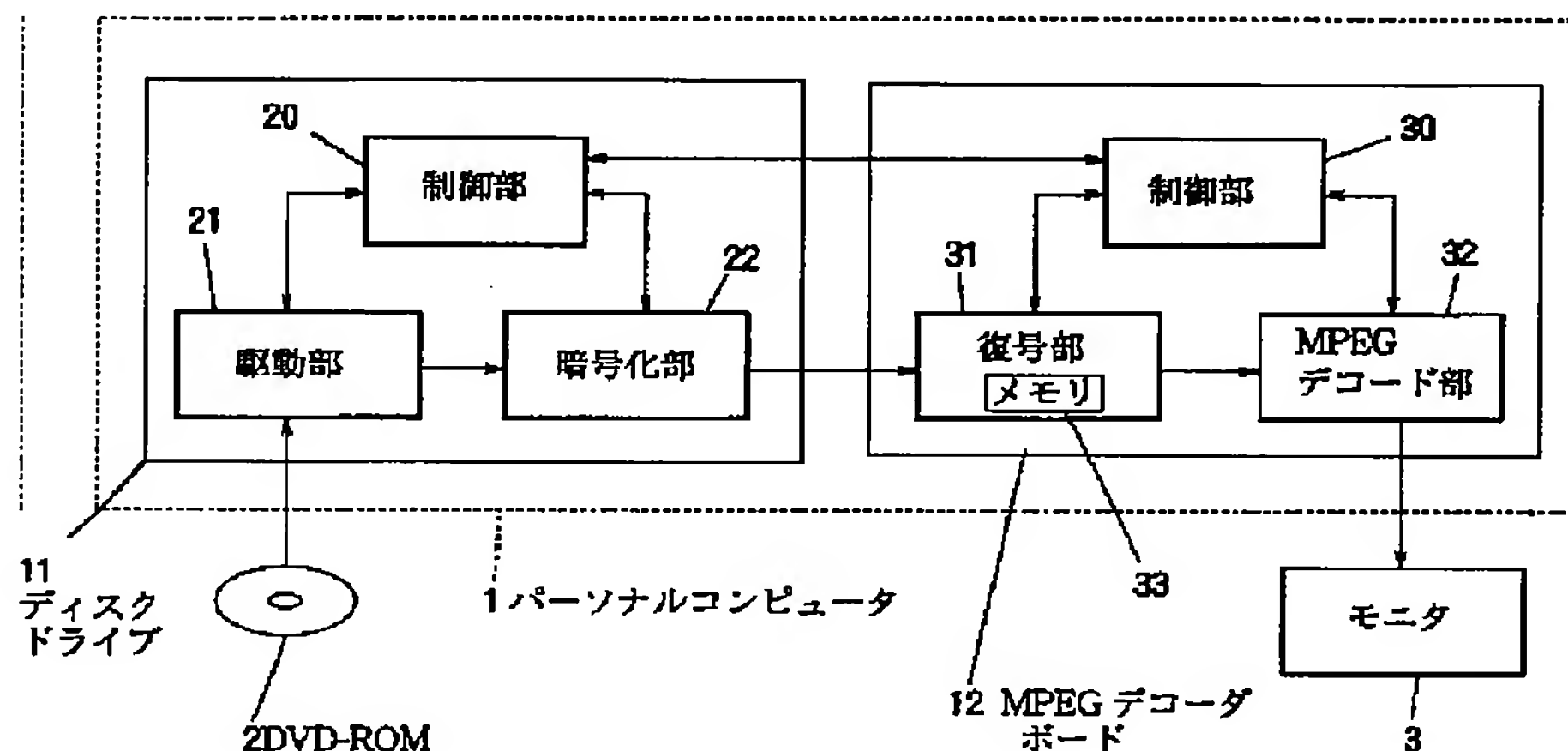
【図12】図8の第2の実施の形態におけるデータの流れを説明する模式図である。

【図13】コンテンツデータを暗号化した場合のキーテーブルの他の例を示す図である。

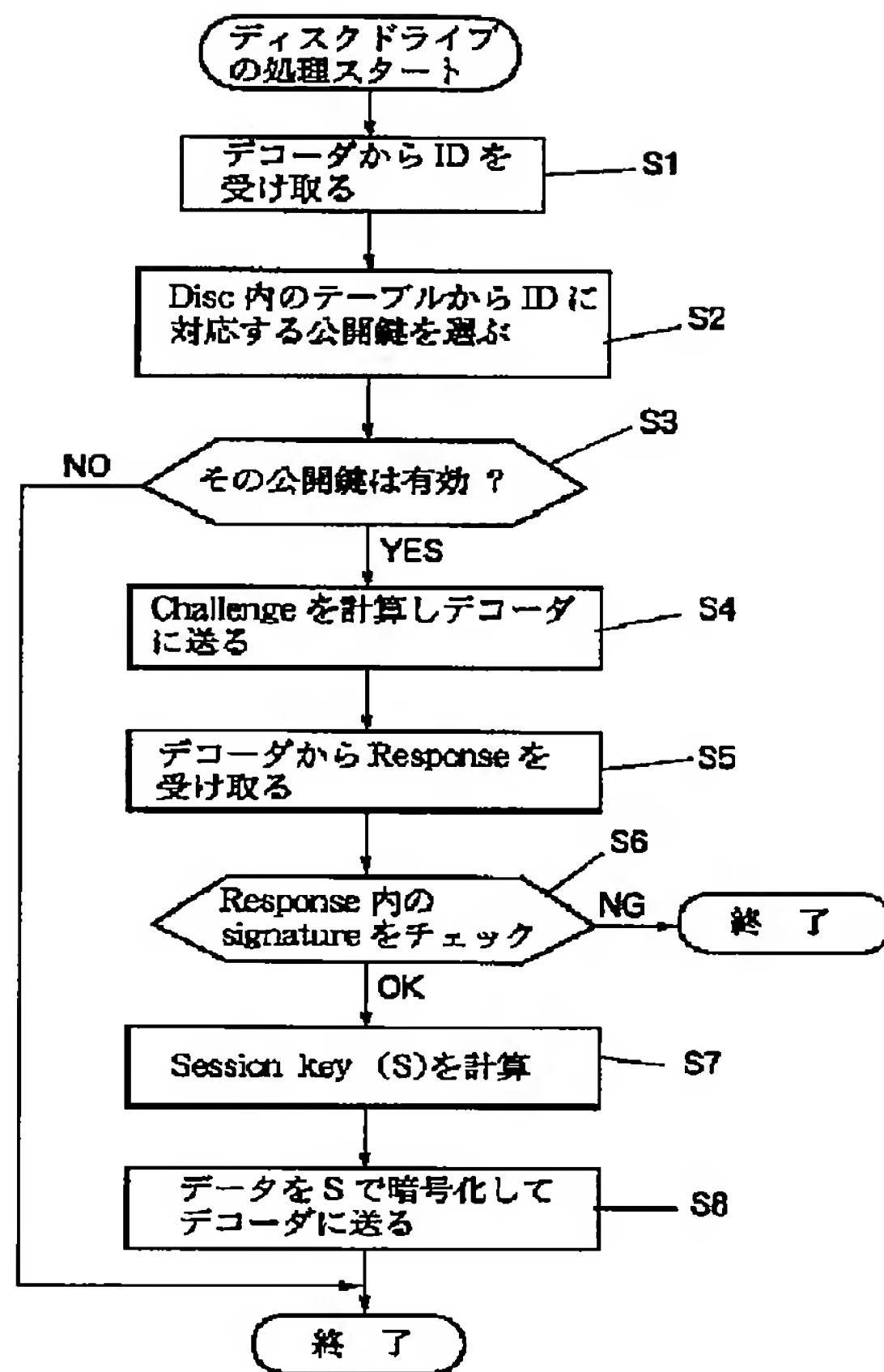
【符号の説明】

1 パーソナルコンピュータ, 2 DVD-ROM, 3 モニタ, 11 ディスクドライブ, 12 MPEGデコーダボード, 20 制御部, 21 駆動部, 22 暗号化部, 30 制御部, 31 復号部, 32 MPEGデコード部, 33 メモリ

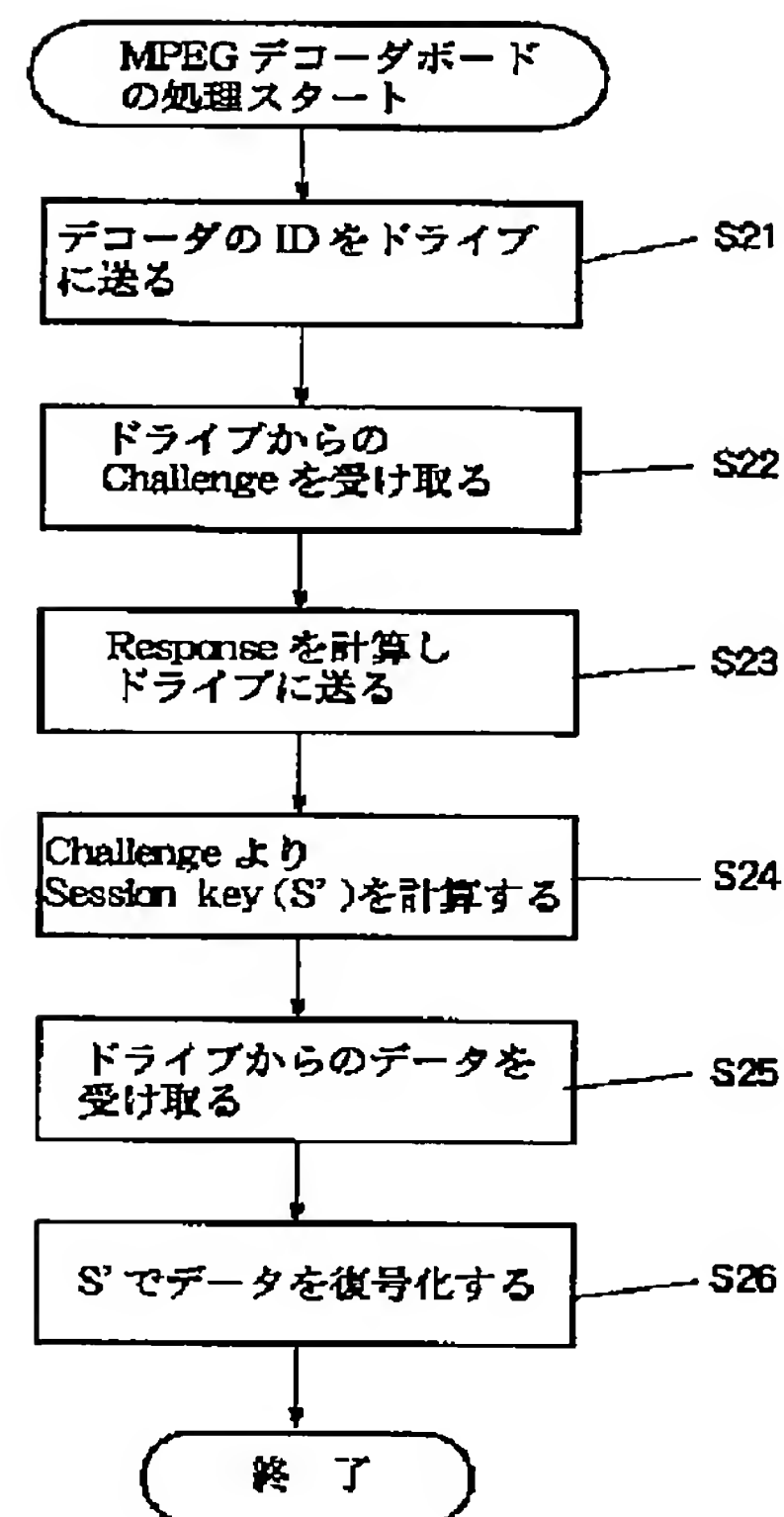
【図1】



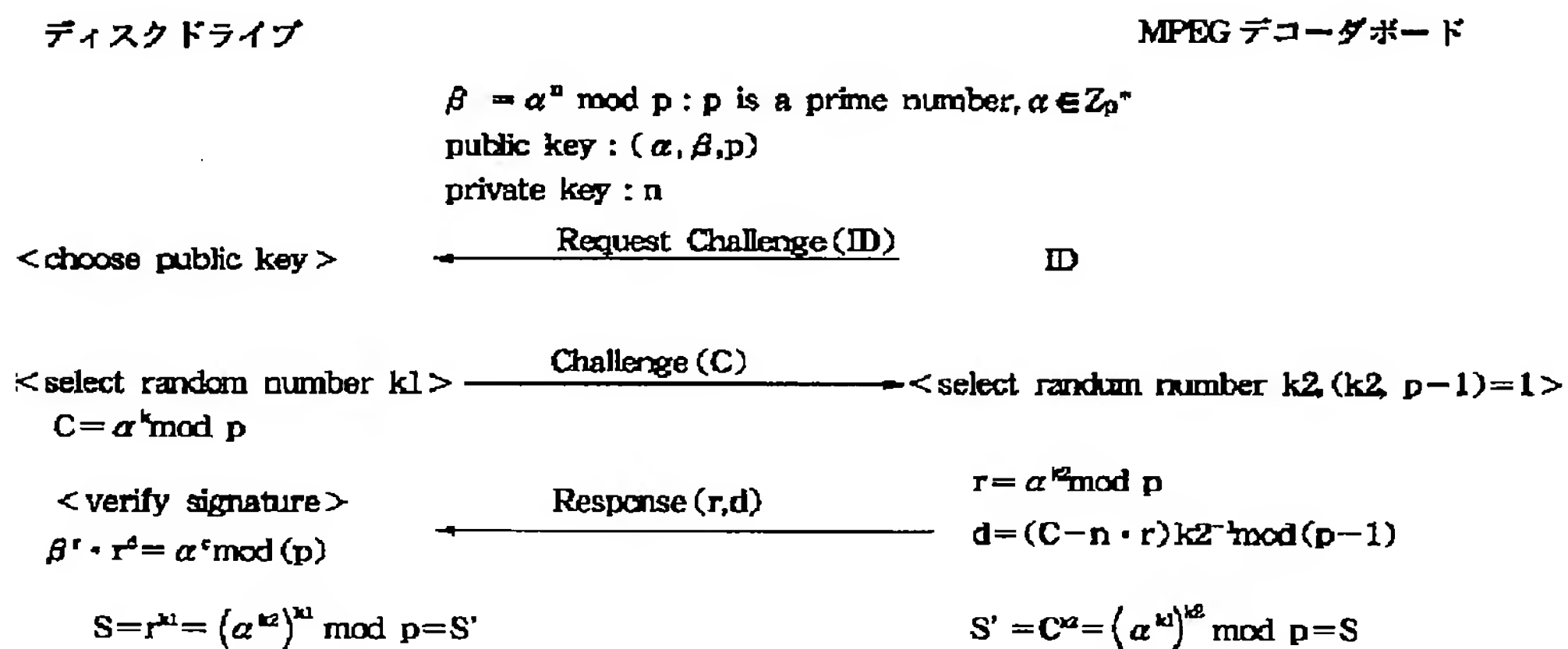
【 図 2 】



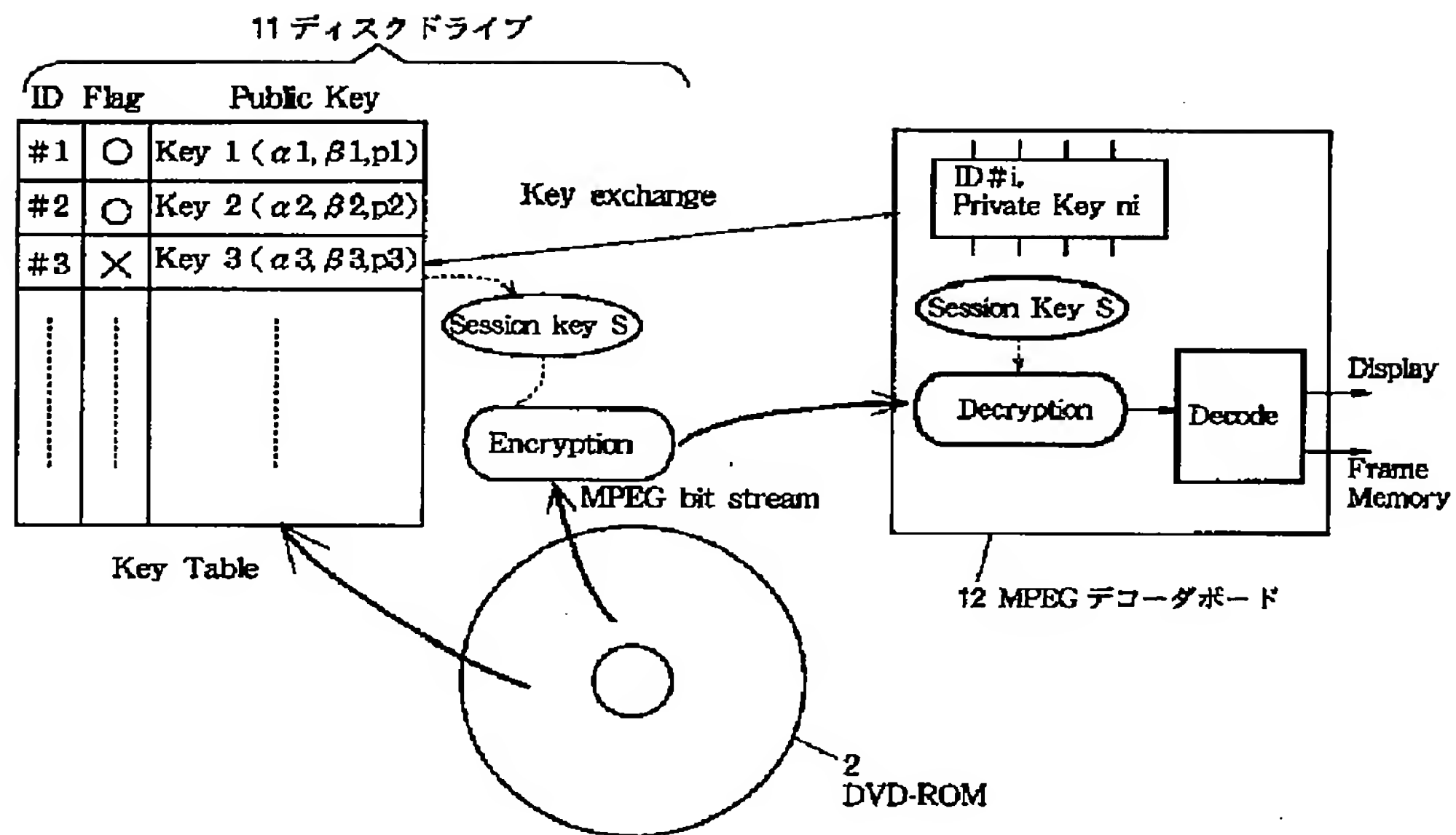
【 図 3 】



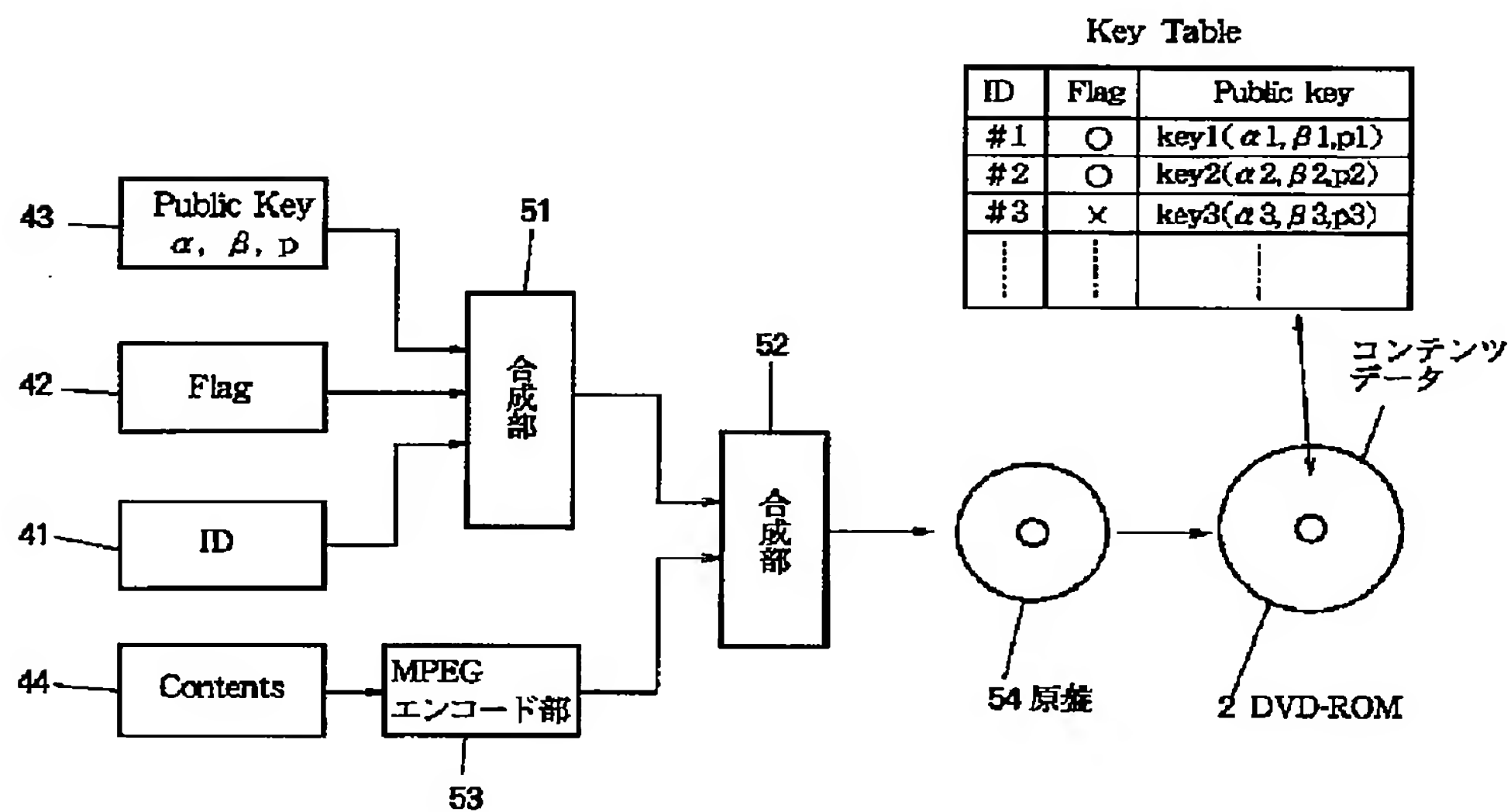
【 図 4 】



【 図 5 】



【 図 6 】

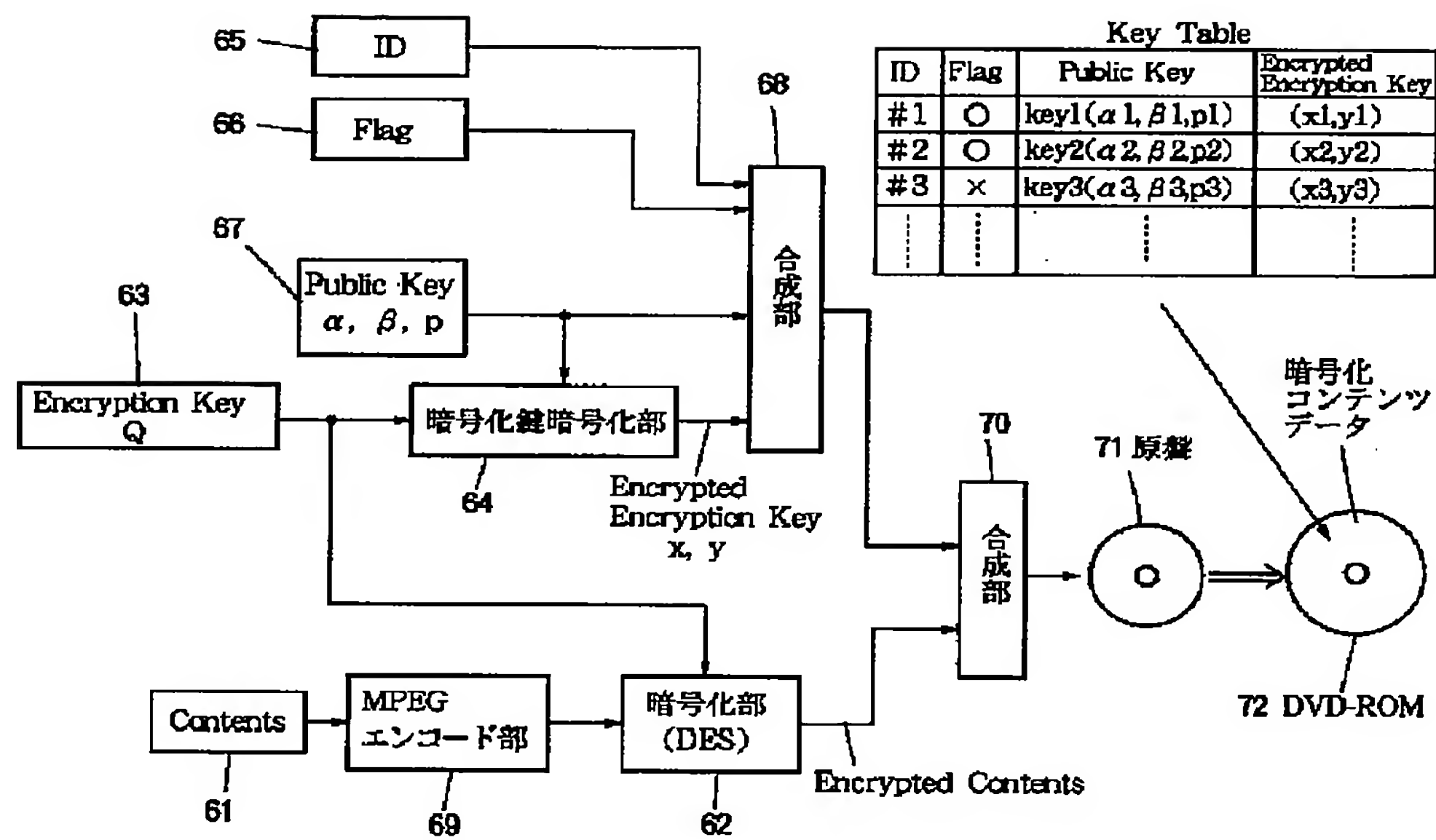


【 図 13 】

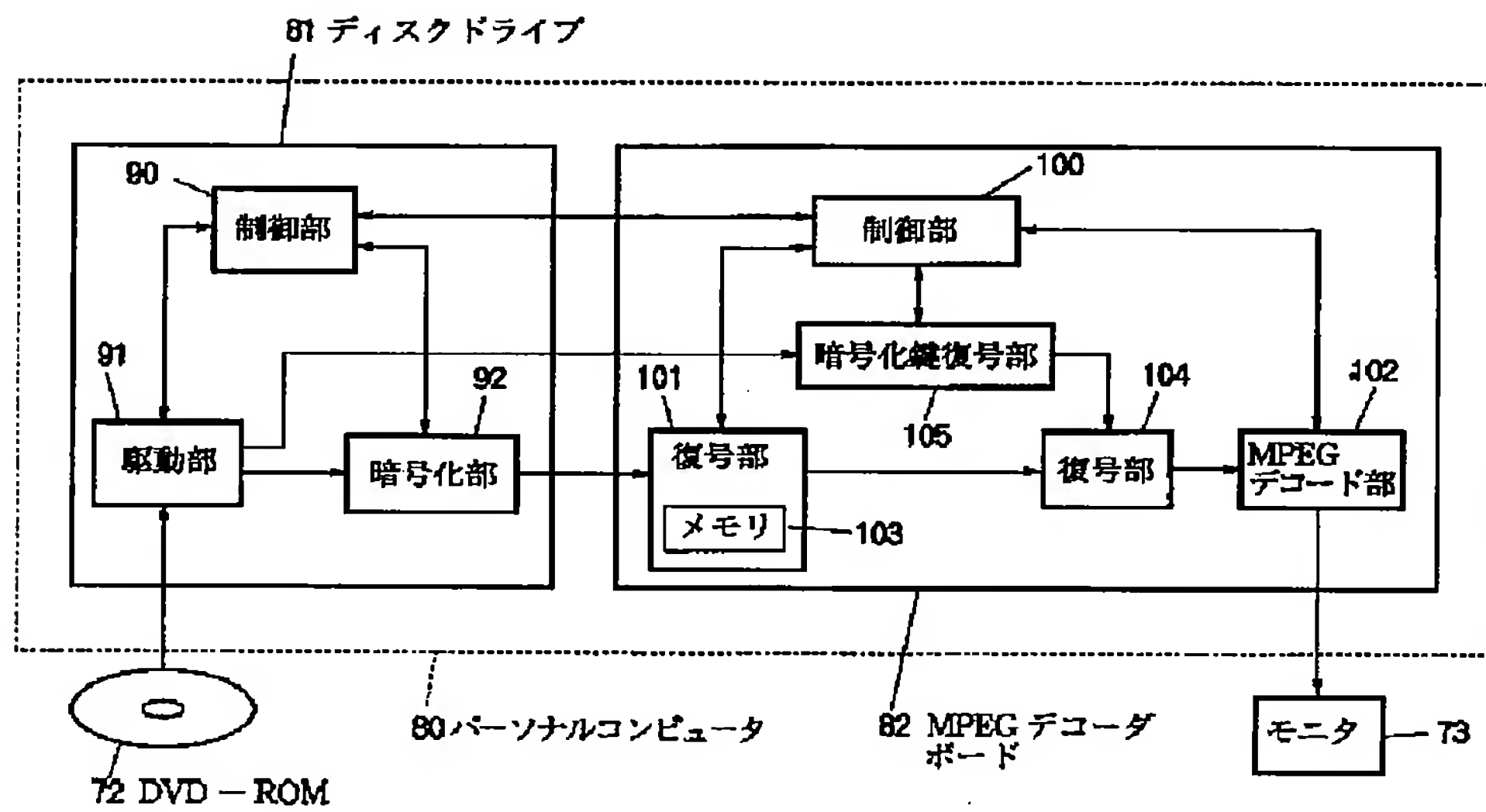
Key Table

ID	Flag	Encrypted Encryption key
#1	○	(x1, y1)
#2	○	(x2, y2)
#3	×	(x3, y3)
⋮	⋮	⋮

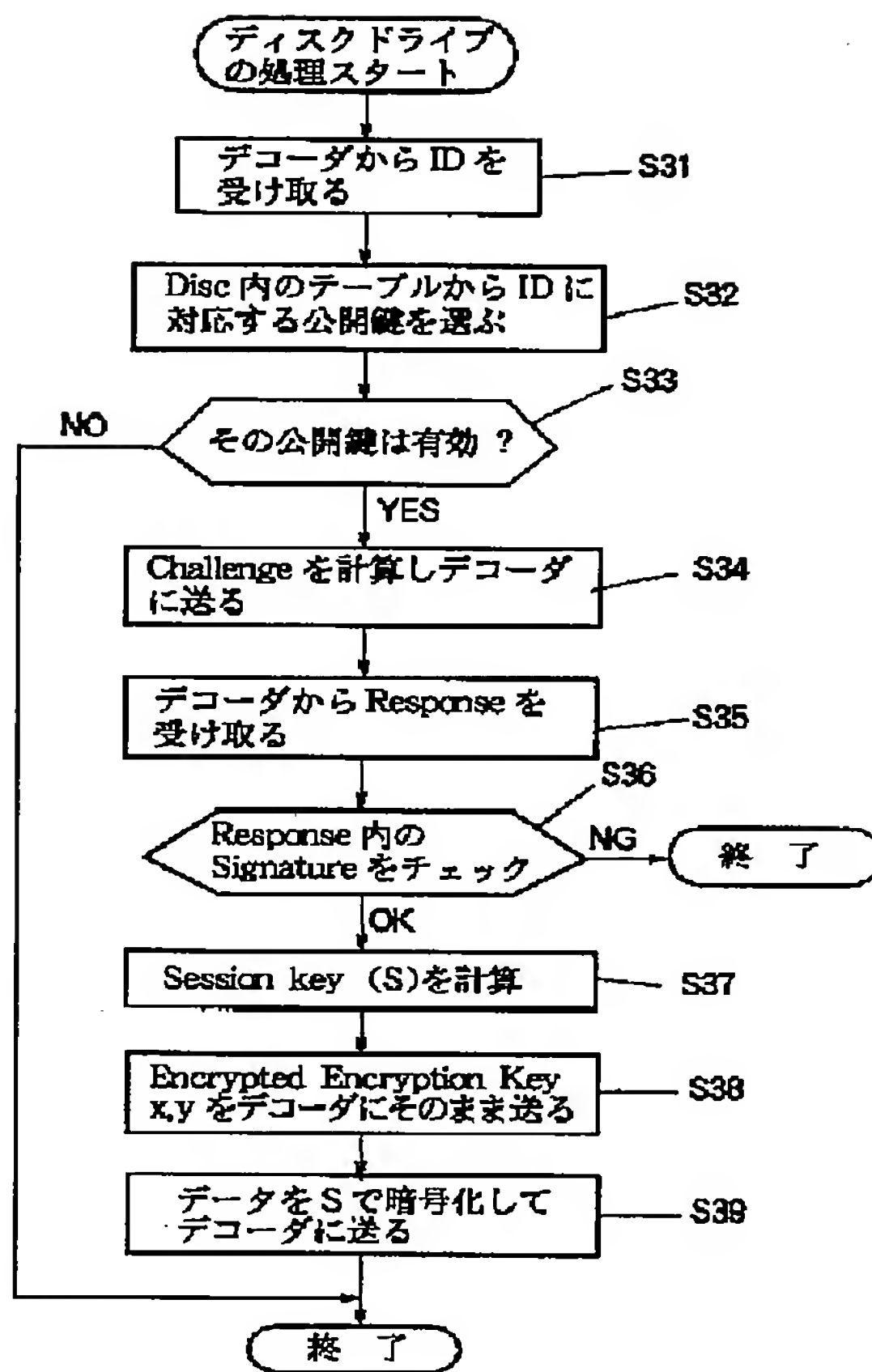
【 図 7 】



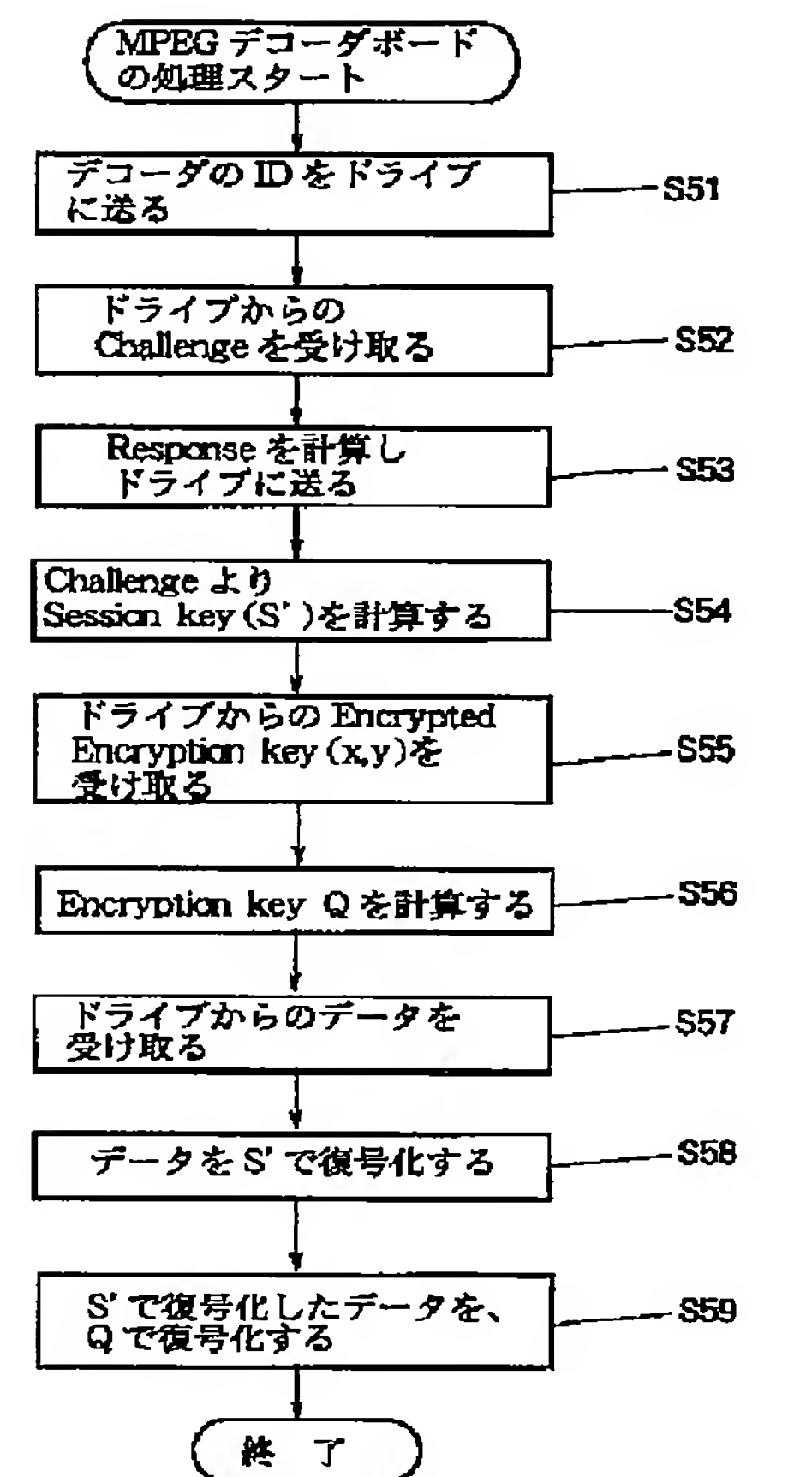
【 図 8 】



【 図 9 】



【 図 10 】



【 図 11 】

ディスクドライブ

MPEG デコーダボード

$\beta = \alpha^n \bmod p$: p is a prime number, $\alpha \in \mathbb{Z}_p^*$
 public key : (α, β, p)
 private key : n

<choose public key>

Request Challenge (ID)

ID

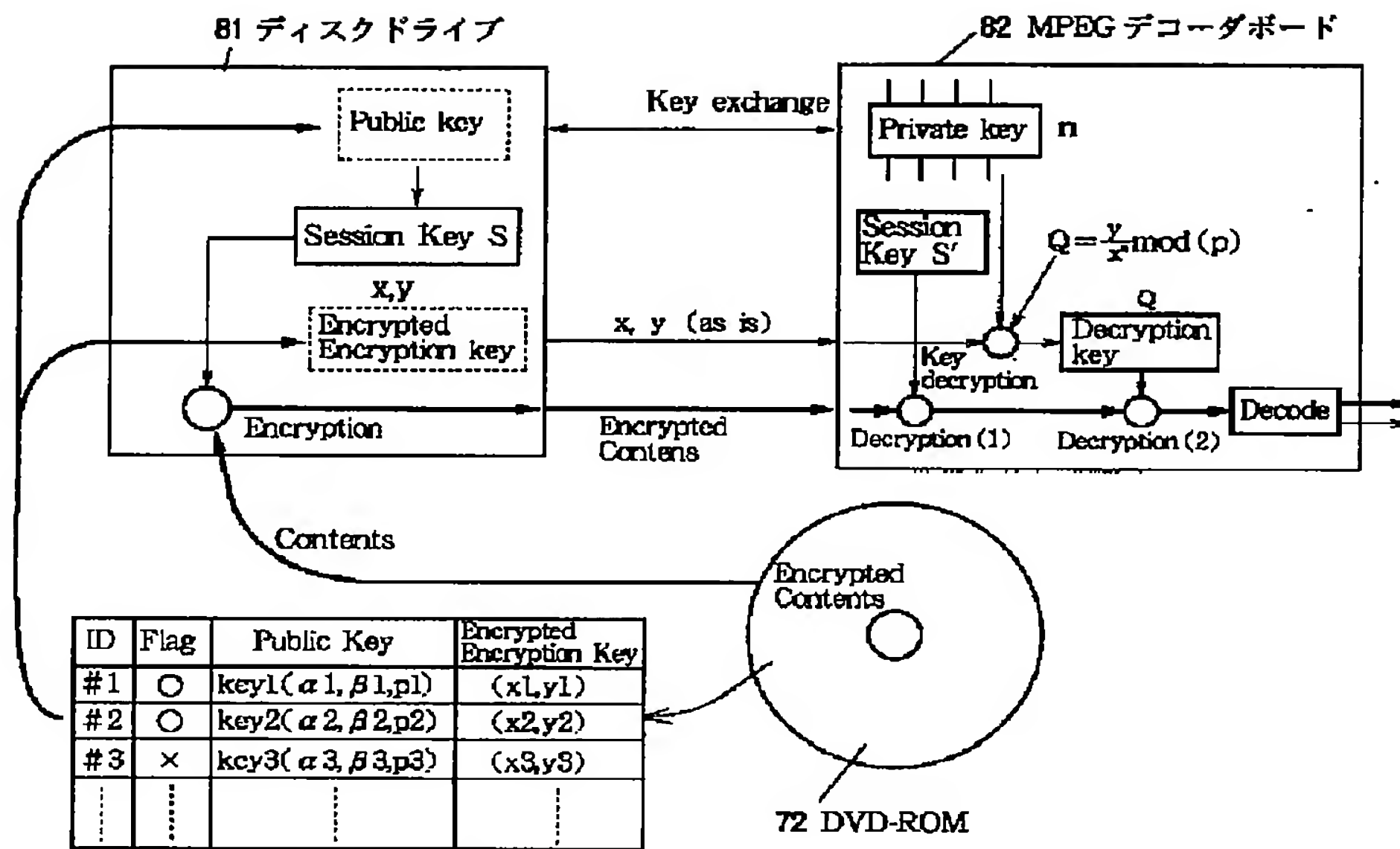
<select random number k_1 > Challenge (C)<select random number k_2 , $(k_2, p-1)=1$ > $C = \alpha^{k_1} \bmod p$

<verify signature>

Response (r,d)

 $r = \alpha^{k_2} \bmod p$ $\beta^r \cdot r^d = \alpha^c \bmod (p)$ $d = (C - n \cdot r) k_2^{-1} \bmod (p-1)$ $S = r^{k_1} = (\alpha^{k_2})^{k_1} \bmod p = S'$ $S' = C^\alpha = (\alpha^{k_1})^\alpha \bmod p = S$ x, y x, y $Q = \frac{y}{x^r} \bmod (p)$

【 図 1 2 】



フロントページの続き

(51) Int. Cl. ⁶

識別記号 庁内整理番号

F I

技術表示箇所

H04N 7/13

Z